**Proof of Concept – Topia**

Topia is a cluster management service.

We are testing the ability of managing and orchestrating a Linux (for now) cluster.

**Table of Contents**

**Subject Page**

Server List…………………………………………………………………………………2

Fields to be assessed…………………………………………………………………2

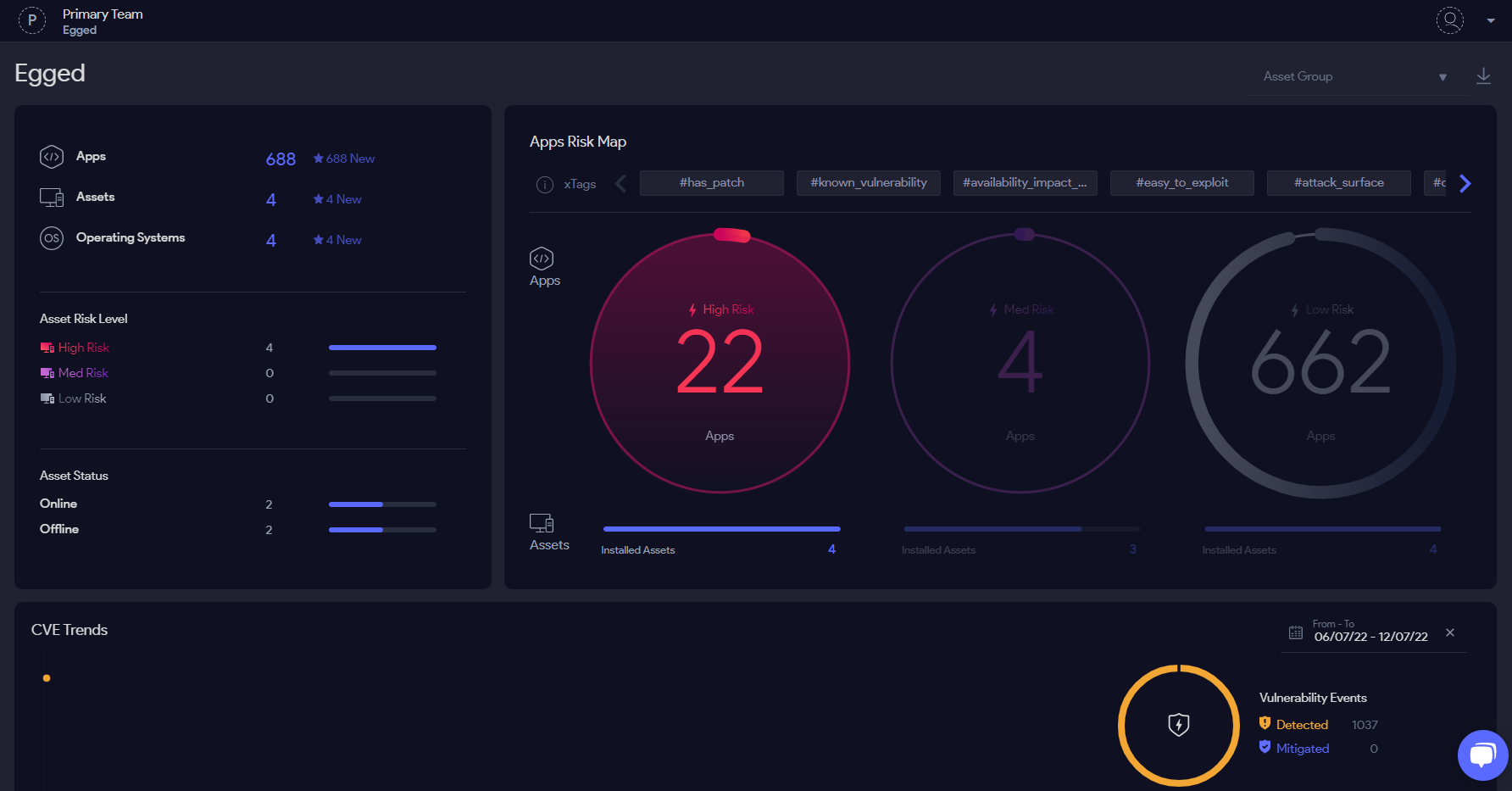
Overview of Topia………………………………………………………………….3-7

Assessment……………………………………………………………………………….8

Servers being tested (data from phpipam):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DNS | IP | Type | Env | OS | Distribution | Dist-version |
| Smslin1-test | 10.0.110.152 | nutanix | TST | Linux | RHEL | 7.6 |
| phpipam | 10.0.110.172 | vmware | PRD | Linux | CentOS | 7 |
| sidurimdev | 10.0.110.230 | vmware | TST | Linux | Oracle | 7.7 |
| devcluster01 | 10.0.100.170 | nutanix | TST | Linux | Ubuntu | 18.04 |
| royg-test | 10.0.110.218 | vmware | TST | Linux | RHEL | 8.6 |

1. Fields to be assessed:
   1. Recognize Operating System (OS) and version
   2. Recognize APPS (python, php, etc…)
   3. Recognize DBs – e.g. Oracle, SQL etc…
   4. Able to perform updates and close security threats.
   5. Able to perform automation tasks, like scripts over multiple servers.
2. Overview of Topia:
   1. Dashboard



You can see the division between the risk levels apps on the right side. And more general info regarding all assets on the left.

* 1. APPS

Graphical user interface, text

Description automatically generated

Lists all apps inside the assets, could be filtered for comfortability.

Was able to recognize oracle, SQL databases.

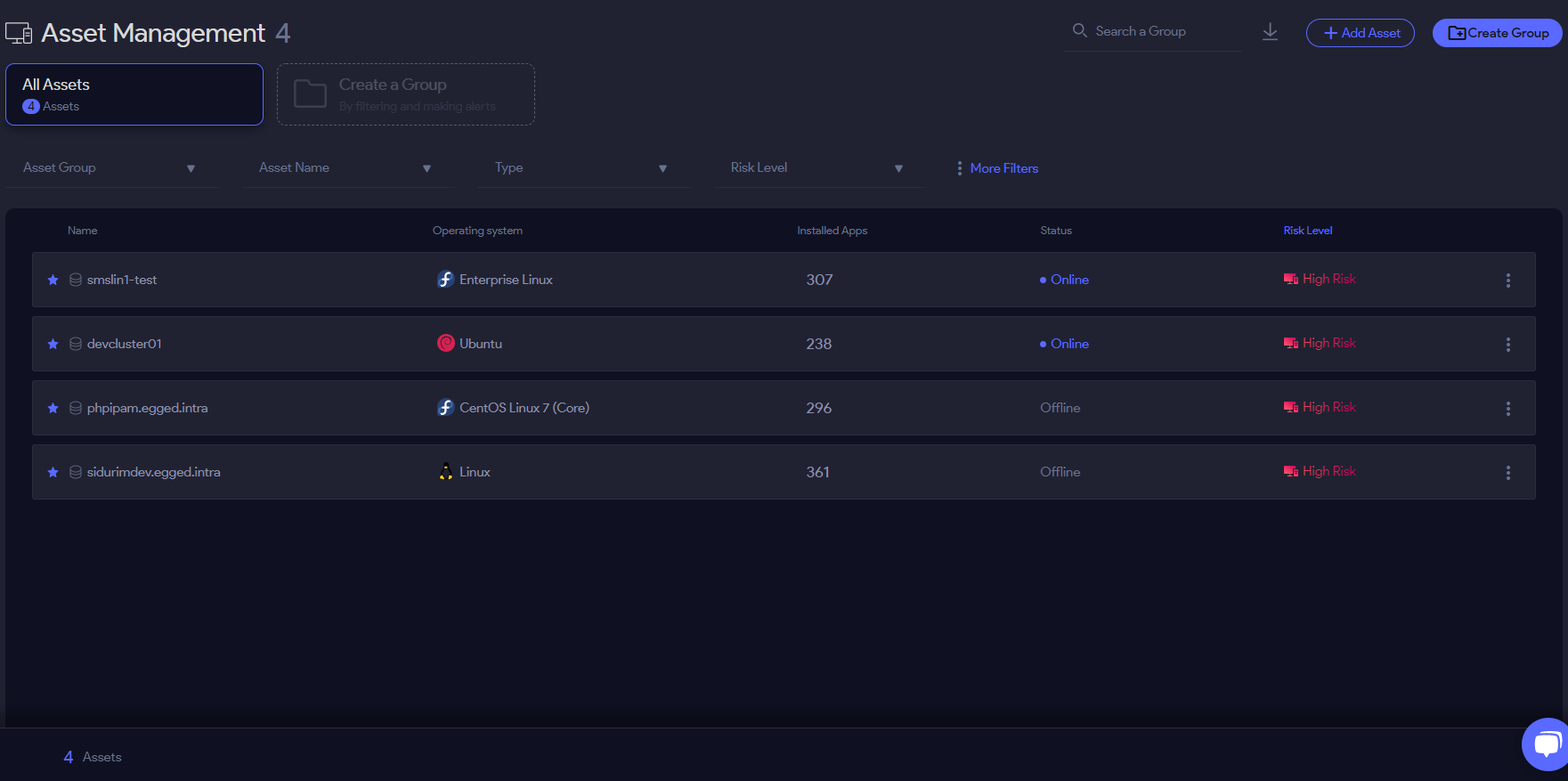
* 1. Operating Systems

A screenshot of a computer

Description automatically generated with medium confidence

Lists OSs and the main updates regarding them.

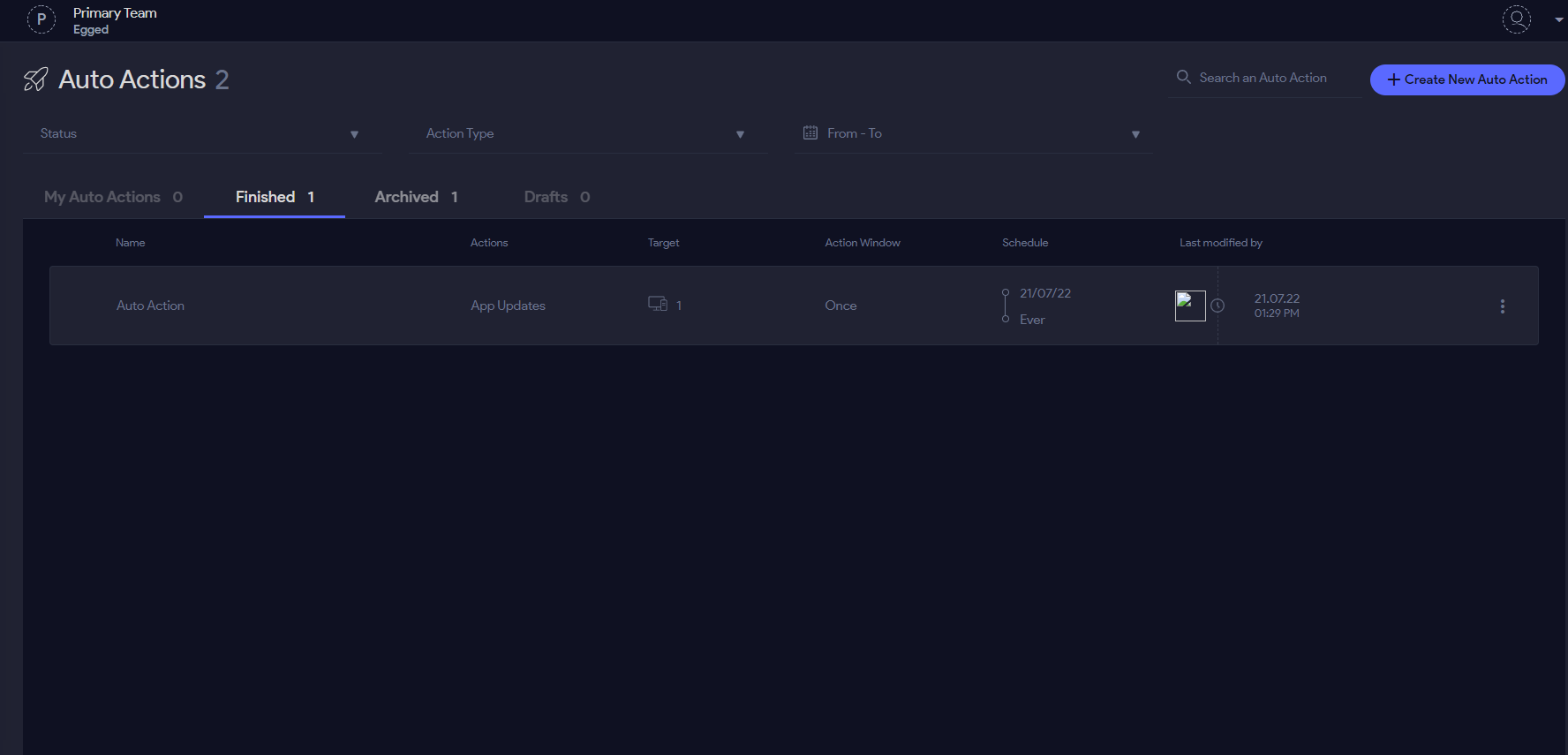
* 1. Assets



Listing the servers connected to the system with the added info:

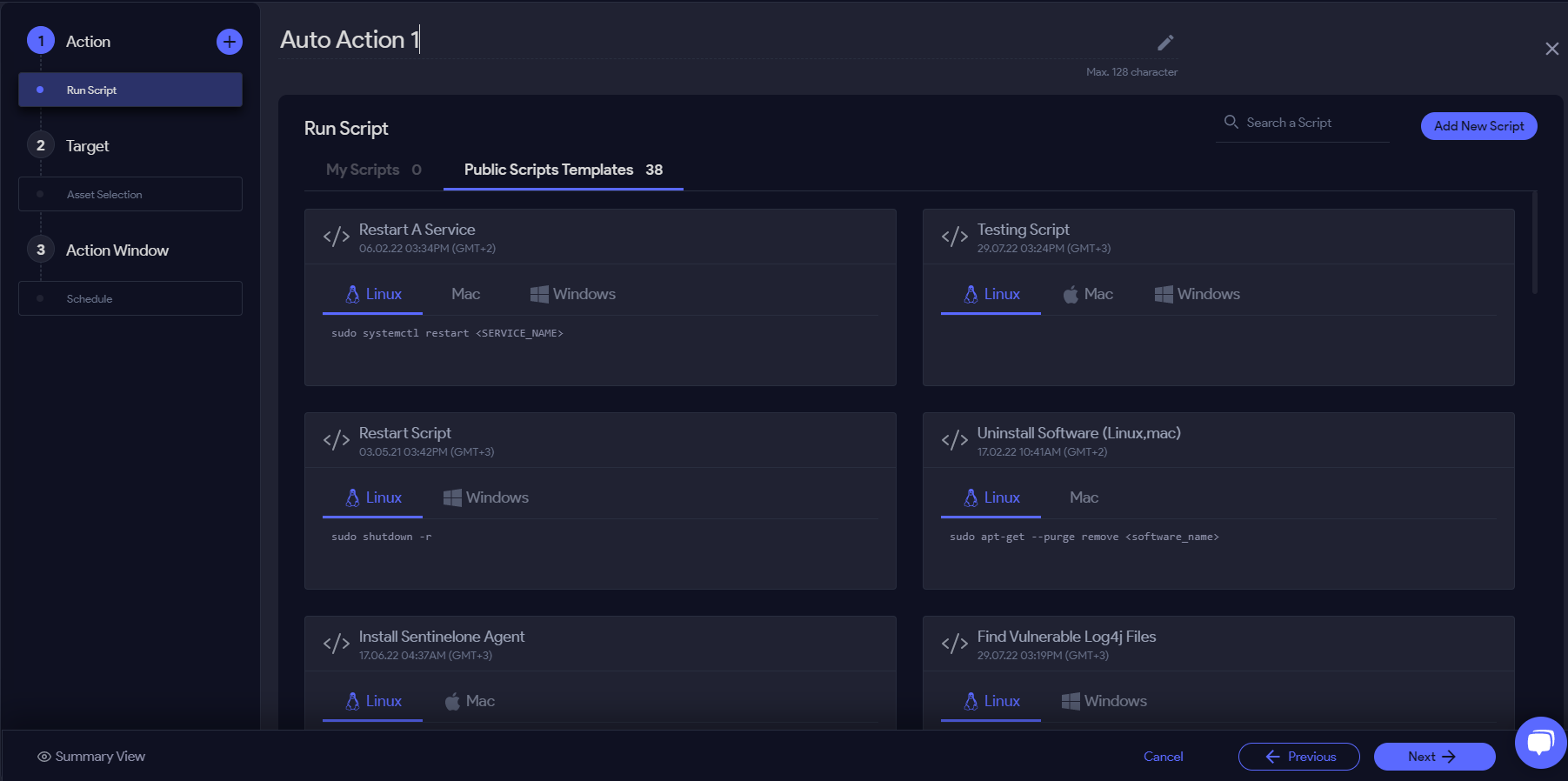
Name, OS, Installed APPS, Status (not accurate), and Risk Level.

* 1. Auto Action



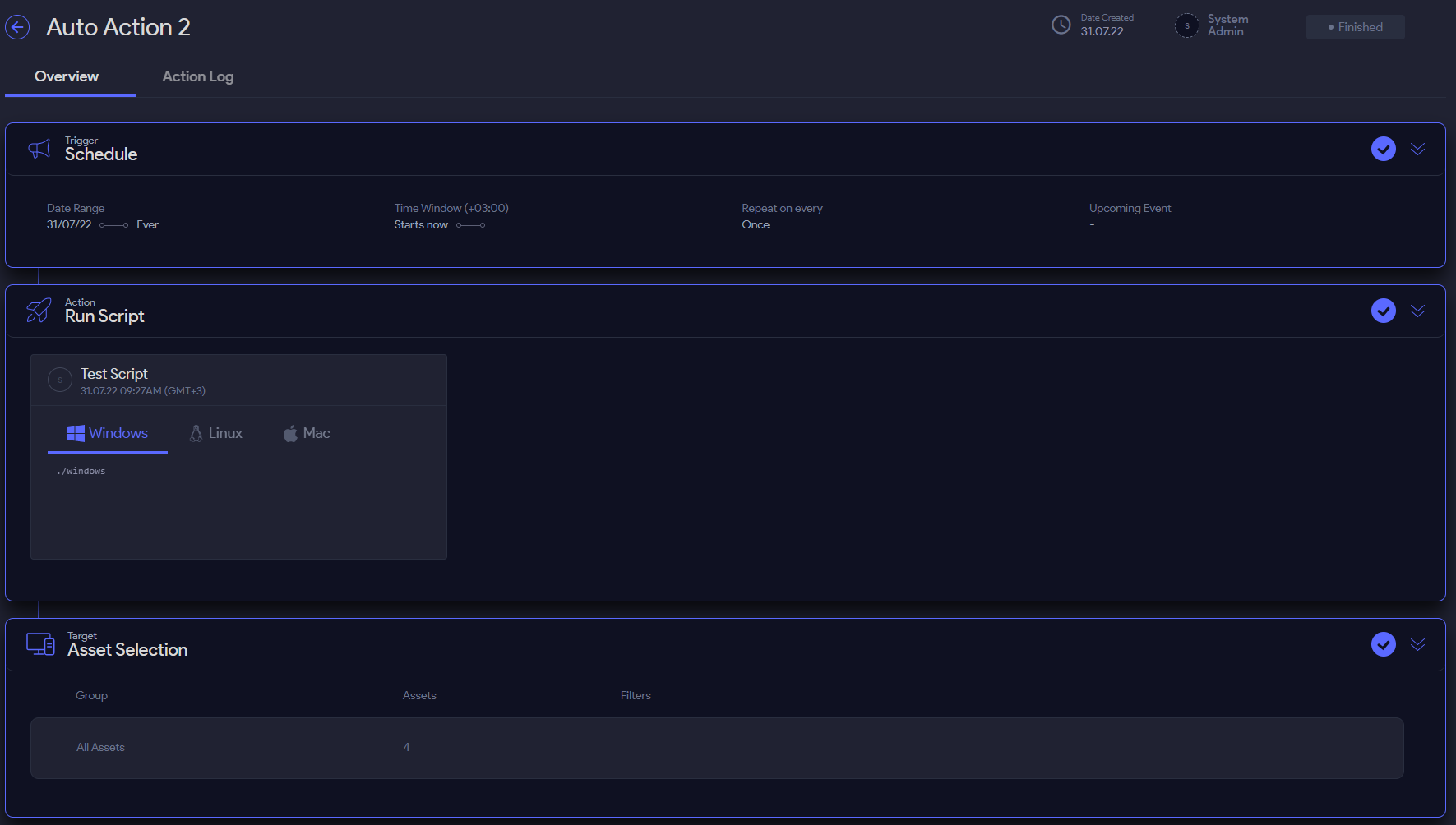
This is where automations could be created to be run on multiple servers.

To run script across several servers simply click on “Create New Auto Action” and then pick “Run Script”:



Here you can see that it is possible to run a variety of different type of codes on a variety of different machines.

Was able to run a simple test script that runs 3 simple commands (pwd, uptime, whoami) in order to check success of execution on all current Linux servers:



A screenshot of a computer

Description automatically generated with medium confidence

It runs scripts as ROOT, doesn’t matter what user you try to connect to TOPIA from.

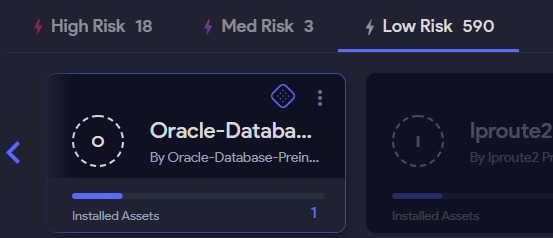
* 1. Patch Management

A picture containing table

Description automatically generated

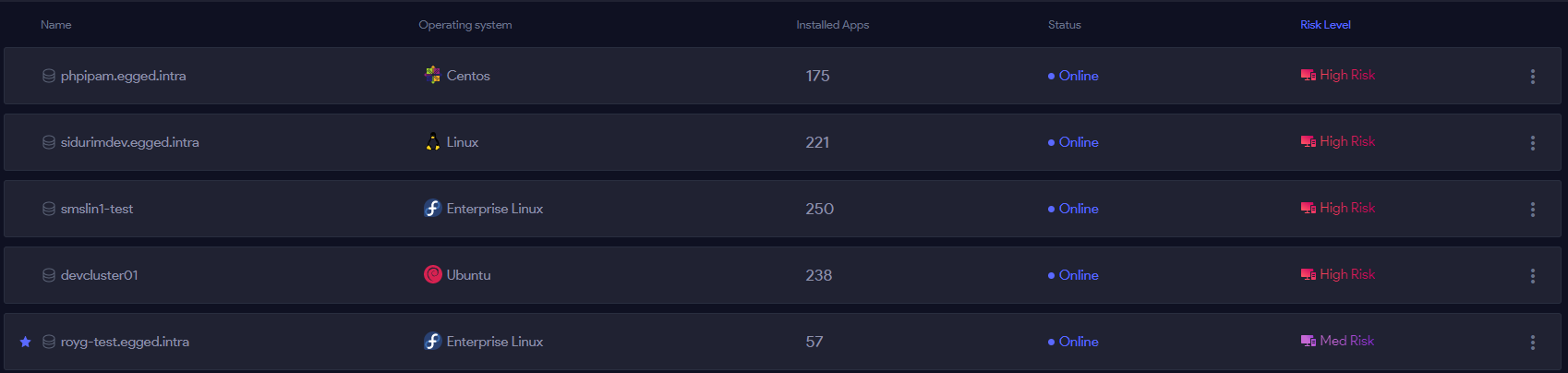
Here you can “Patch”/update APPS or Oss (kernels) across several machines.

1. Assessment:
   1. Recognize Operating System (OS) and version – SUCCESS
   2. Recognize APPS (python, php, etc…) – SUCCESS
   3. Recognize DBs – e.g. Oracle, SQL etc… - SUCCESS



It was able to recognize oracle-DB SQL-DB.

* 1. Able to perform updates and close security threats. – SUCCESS



After updating all apps in the server, I made sure that the updates actually happened inside the server.

And after patching all “HIGH RISK” threats on the same server, I was able to lower the “Risk Level” to “Med Risk” instead of “High Risk”

* 1. Able to perform automation tasks, like scripts over multiple servers. - SUCCESS